Research Proposal of the Thesis Entitled

CYBER ECONOMIC CRIMES IN INDIA: DECODING CYBER CRIME INVESTIGATION, RESTITUTION OF VICTIMS AND ITS PREVENTION

Submitted for the award of the Degree of

Doctor of Philosophy

by

Divyam Jhaveri

(Enrollment Number: 202003004)

Under the guidance of:

Dr. Aseem Chandra Paliwal,
Associate Professor (Law)

Unitedworld School of Law

KARNAVATI UNIVERSITY

Karnavati University, Gandhinagar

Introduction

The advancement of information technology has had a profound impact on the global economy, revolutionizing the way people and markets are connected. The internet has ushered in an era of hyper-connectivity, making information sharing between individuals across borders quick and effortless. This has resulted in the creation of a borderless cyber-world marked by instant communication.

Information technology has given rise to a virtual world where activities such as information exchange, communication, and high-value transactions that used to take weeks or months can now be completed almost instantaneously. This advancement has facilitated the growth of e-commerce, virtual communities through social networks, online education, entertainment, and other essential services. Although these activities have generally had a positive impact on society, there are also individuals who exploit the internet to perpetrate various cybercrimes. The internet has globalized the crime scene, as cybercrimes know no borders.

One prevalent form of cybercrime is cyber economic crime, which has gained a significant foothold in the cyber world. With India's aspirations of becoming a digital economy, the increasing threat from cyber economic crime is alarming. Consumers are enticed by the convenience, competitive prices, and personalized experiences offered by online retail, but this has also led to a rise in digital fraud. Instances of fraud and large-scale data breaches affecting thousands of users have been reported.

Consumers can now order services and products and have them delivered to their office or home with just a few clicks or voice commands on their mobile phones or computers. Consequently, the use of electronic payments has surged in India, leapfrogging the reliance on physical cards. The Reserve Bank of India predicts a significant increase in digital transactions from December 2018 to December 2021. The e-commerce market in India, worth USD 50 billion in 2018, is expected to reach USD 200 billion by 2026. **C**onsidering the above, the exponential rise in cyber economic crime is a certainty. Therefore, the researcher aims to analyze new forms of cyber economic crime, the role of law enforcement agencies, the need for investigative tools and procedures, cyber security best practices, and effective approaches to support victims of such crimes.

Statement of Research Problem

It is widely known that the ongoing process of digitalization is inevitable, and with the widespread use of internet-based technology, there is an urgent need to address the concerning increase in cybercrime cases, particularly in the realm of online financial fraud.

It is of utmost importance to establish a swift and action-oriented system that addresses grievances and ensures the recovery of lost funds. The gravity of the issue demands immediate attention due to the substantial amount of public funds involved. As we enter the era of digitalization, a significant portion of government and citizens' money is at risk of being exposed to cyber fraud. Therefore, it is vital to conduct research and develop policies based on successful international experiences in the areas of cybercrime investigation and prevention.

The current state of affairs, characterized by increased unemployment and financial instability during the COVID-19 pandemic, has significantly contributed to the surge in cybercrime rates. This claim is supported by the findings from the INTERPOL Global Cybercrime Survey conducted between April and May 2020, which clearly indicates a disturbing rise in cybercrime cases worldwide.

Literature Review

- **Nandan Kamath (2012)**, within this book, the author delves into the untapped potentials and incredible advancements of cyberspace, along with the profound impact it has had on human existence. Additionally, the author critically examines the diverse legal considerations that govern this digital realm, including a thorough analysis of the Indian Information Technology Act, 2000. The author expressly advocates for a minimalist regulatory framework, wherein the advantages of the Information Revolution can be realized in a harmonized manner, while cautioning against the hazards associated with excessive regulation.
- **Mohamed Chawki, Ashraf Darwish, Mohammad Ayoub Khan, SapnaTyagi, (2015)**, this book is part of the esteemed Series "Studies in Computational Intelligence (SCI)" published by Springer International Publishing Switzerland, which presents cutting-edge developments and advancements in various fields of computational intelligence. The research presented within the book is based on comprehensive analysis of real-world incidents, particularly in the United States and the United Kingdom. It explores the complex landscape of cybercrimes and the management challenges they pose. To undertake this analysis, multiple sources are utilized, reflecting the decentralized nature of the Internet that often generates diverse and sometimes contradictory information pertaining to cybercriminal activities and their impact on victims. The book elucidates the ways in which cybercriminals exploit the Internet as both a tool and a platform, with specific focus on the problem of phishing and the illicit use of stolen financial information. Additionally, it carefully examines the concept of Internet anonymity,

considering its significance as a conduit for freedom of expression while balancing the imperative of user privacy with national security concerns.

- **Vakul Sharma (2010)**, in this book, the author provides a comprehensive and detailed analysis of the legal aspects related to Information Technology, specifically in alignment with the Information Technology Act of 2000. The author meticulously scrutinizes the key chapters of this Act and critically examines the challenges encountered during its practical implementation. Moreover, the author extensively explores the principles that govern jurisdictional issues in cyberspace, encompassing aspects such as passive personality, territoriality, universality, effect, and the protective principle. The book presents an in-depth analysis of the legal framework, supplemented by a thorough discussion of landmark judicial decisions pertaining to cyberspace.
- **Dr. Vishwanath Paranjape (2010)**, this book centres around exploring the origins of cybercrime and the significant growth of cyber space crime, driven by the increasing reliance on Information technology. The author undertakes a comprehensive analysis of the legal framework in India concerning cyber space, meticulously examining the preventive laws and measures implemented to combat the pervasive threat of cybercrime. Additionally, the author extensively discusses the imperative of establishing a robust national and international cooperative mechanism to effectively address the global issue of cybercrime. Accordingly, the book proposes a comprehensive policy framework for dealing with cybercrimes, considering the complexities and challenges they present in today's interconnected world.
- **Pawan Duggal** (2013), in this book, the author provides an extensive analysis of the complex issue of cybercrime, delving into the hidden world of the dark web and uncovering its potential to cause significant harm beyond initial expectations. The author adopts a unique perspective, recognizing the evolving and dynamic nature of cybercrime, and emphasizes the need for a flexible jurisprudence in cyber law to effectively address this ever-changing problem. The author suggests that the legislative framework and implementation should allow for swift changes and adaptations. Furthermore, the book comprehensively and clearly elucidates the emerging developments in cyber law and their legal consequences. It also explores preventive mechanisms aimed at comprehending the phenomenon of cybercrime and safeguarding against its detrimental effects.

- **Nidhi Saxena** (2017), within this book, the author provides a comprehensive overview of the established facts and concepts surrounding cybercrime, while also analyzing the regulatory challenges it presents to the criminal justice system. Recognizing the ever-evolving nature of cybercrime, the book highlights the need for qualified assumptions in its detection, forming the basis for redefining and categorizing cybercrime. Subsequently, the author proceeds to examine the prevailing trends of cybercrime at the state level in India. These trends are evaluated through various criteria such as age demographics, motives behind the crimes, cases registered under the Indian Penal Code, and other pertinent factors. Through this analysis, a refined understanding of cybercrime in the Indian context is developed, offering valuable insights into its nature and impact.
- **Dr. Amita Verma** (2009), within this book, the author presents a comprehensive exploration of the concepts of cybercrime, its essential components, and its classification based on various parameters. Throughout the book, cybercrime is depicted as a grave global epidemic that poses significant challenges in the current millennium. The author emphasizes the need for a balanced approach that optimizes the use of cyberspace while concurrently minimizing cybercrime. Additionally, the book highlights the crucial role of both national and international judiciary in combating the proliferation of cybercrimes, as well as the legislative approaches required to address the complexities of civil and criminal liabilities pertaining to cybercrimes in today's world. Moreover, the author thoroughly examines the obstacles faced by the criminal justice system due to the rise of cybercrimes. By effectively delineating the relevant legal provisions pertaining to cybercrime, the book concludes by offering insightful suggestions aimed at promoting sustainability in the cyberspace and effectively addressing the issue of cybercrime when implemented.
- **Dr. M. Dasgupta** (2009), this book focuses on conducting a comparative examination of the laws pertaining to different types of cybercrime in India, the United States, and the United Kingdom. The various types of cybercrime discussed encompass hacking, cyber fraud, cyber pornography, and cyber terrorism, among others. The author elucidates the intricate nature of classifying cybercrime, given its status as a continuously expanding domain of criminal activity. Within the book, cybercrime is classified into three categories: crimes where the computer serves as the victim, crimes where the computer is incidental to other criminal activities, and crimes associated with the widespread use of computers. Following an exploration of the relevant legal provisions, the author provides

recommendations that cater to the needs of students, research scholars, academicians, and other members of the legal community. These recommendations serve to enhance understanding and facilitate further research in this field.

- **Dr. Talat Fatima**, (2016), in this book, the author provides a detailed exploration of cybercrime as a departure from traditional forms of criminal activity, emphasizing the evolution of criminal law, the criminal justice system, cybercrimes, and their classification. The comparative study of laws between the United States, the United Kingdom, and India is presented, recognizing the technological and legal advancements of these nations. The book also addresses the need for establishing a foundational framework to effectively prosecute cybercriminals, particularly in India where a comprehensive legislation for cybercrimes is lacking. Additionally, the analysis delves into the legal complexities arising from the presence of foreign elements in the cybercrime landscape. The author concludes that cybercrime transcends national borders and lacks allegiance to patriotism, humanism, and traditional jurisprudence. Consequently, the laws governing cybercrimes need to evolve in tandem with the international nature of this phenomenon. The recommendations put forth in the book primarily focus on substantive criminal law and procedural law, aiming to address the unique challenges posed by cybercrime.
- **Swati Mehta** (2016), this paper focuses on the challenges encountered by the Judiciary when considering the admissibility of electronic evidence, in accordance with Section 65B of the Indian Evidence Act. It also integrates the role of cyber forensics in the process of confiscating, preserving, and presenting electronic evidence. Moreover, the paper provides a thorough examination of the procedures involved in handling, preserving, and presenting electronic evidence in court. It aims to offer valuable suggestions to enhance the reliability and efficiency of this process.
- **Ranjit Singh**, (2017), in this paper, the author conducts a critical analysis of the global threat posed by cybercrime and emphasizes the urgency to address this menace. The paper also highlights common challenges faced in tackling the issue of cybercrimes. Furthermore, the author strongly advocates for the establishment of a comprehensive global legal framework to regulate cyberspace. This would require coordinated efforts from all countries and international organizations in order to effectively combat cybercrime.

- **Raveena Rai**, (2015), In this paper, the author sheds light on the distinctive investigative approach required for cybercrime as opposed to traditional crime investigation. The paper discusses the underlying reasons for this differential approach, such as jurisdictional challenges, inadequacy of existing laws, concerns regarding data privacy, and other related issues. Additionally, the paper presents a comparative analysis of cyber investigation systems worldwide and proposes necessary reforms for the Indian context. By examining the global landscape, the author offers valuable insights and recommendations to enhance the effectiveness of cybercrime investigations in India.
- **Angkasa**, (2018), in this paper, the author endeavors to present a socio-legal empirical investigation into cybercrime victims, emphasizing the crucial requirement for robust legal protections for these individuals. The author also examines the concept of victim precipitation within the realm of cybercrime and advocates for the implementation of stringent legal regulations that mandate appropriate preventive measures against cybercrimes.
- **Mohit Kumar,** (2020)**, t**his journal article, published in the International Journal of Forensic Sciences, presents an overview of the current state of digital forensics and cyber security in India. It delves into the challenges faced by law enforcement agencies, including the legal and police departments. The article also provides a brief analysis of the prevailing trends and patterns in digital forensics and cyber security within India. The primary objectives of this research paper revolve around studying digital forensics in the context of the rules and legislation enacted by the Indian parliament, as well as their implementation by the police and judicial systems. The article aims to identify any ambiguities that may exist within these regulations. Additionally, the article seeks to explore the role of ethical hackers and how their knowledge and expertise can contribute to strengthening India's cyber security measures and the evolution of digital forensics in the country.
- **Jayanto Narayan Choudhary,** (2020), this research article is featured in the Special Issue on Internal Security of The Indian Police Journal, which is published by the Bureau of Police Research & Development (BPR&D). As a peer-reviewed journal, it covers various topics pertaining to policing, internal security, and related subjects. The article extensively explores the transformation observed in the policing system over the past 50 years, stressing the necessity of revolutionizing this system to effectively address present-

day challenges. It underscores the importance of meticulous attention to criminal research, training, and scientific investigation of crimes.

- **Aloka Prabhakar**, (2020), this research article introduces the innovative concept of Fifth Generation Warfare (5GW), which employs cognitive exploitation tactics. It examines the significant increase on the internet and social media's influence as tools for engaging in information warfare. The paper proceeds to explore the intricacies of 5GW, leading to a paradigm shift in cybersecurity, and the emergence of cyber threat intelligence (CTI). These models are designed to safeguard national security by protecting critical assets and the information space from deliberate contagion. The research article is part of a Special Issue on Internal Security published in April-June 2020, within The Indian Police Journal. It is one of twelve articles featured in the issue, covering various topics such as the analysis of internal security, terrorism, insurrection, leftist extremism, and the causes and consequences of radicalization.

Further Literature Review: Reports

1. Reserve Bank of India, 'Report of Working Committee on information security, electronic banking, technology risk management and cyber frauds' (2010). *https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WREB210111.pdf*

   This report focuses on the imperative of fortifying the Information Technology infrastructure within the banking system of India, considering the persistent rise in cyber frauds and the associated challenges in cyber security. The report has been prepared by a Working Group of Professionals convened by the Reserve Bank of India, headed by the former Executive Director, Shri G. Gopalkrishnan. The report comprehensively addresses key aspects pertaining to Information Technology Governance, combating cyber frauds, analyzing technology risk management, and the critical need for robust Cyber Security measures. Through its analysis, the report highlights the significance of strengthening the Information Technology infrastructure within India's banking sector to mitigate cyber threats effectively.

2. A DSCI-PayPal Joint Study, Fraud & Risk Management in Digital Payments, August 2020. *https://www.dsci.in/sites/default/files/DSCI-PayPal-Report.pdf*

   This report centers around formulating strategies to address the escalating prevalence of online financial frauds and cyber economic crimes in India, driven by the growing digitization and online payment systems. As a result, it undertakes a comprehensive examination of emerging online financial frauds, potential threats within the payment system, the importance of

implementing enhanced fraud prevention strategies, and an analysis of recommendations for various stakeholders. The goal of this study is to provide a holistic approach to mitigating these challenges and promoting secure online transactions in the evolving digital landscape.

3. INTERPOL's Cybercrime Directorate, 'Cybercrime: COVID-19 Impact' (2020)

   This report, published by INTERPOL's Cybercrime Directorate, evaluates the global landscape of COVID-19 related cybercrimes. Drawing on a meticulous analysis of data collected from 194 member countries and private partners, the report offers a comprehensive overview of the prevalent cybercrime trends in the context of the ongoing pandemic. In great detail, this assessment report outlines how cybercriminals have employed tactics such as sending COVID-19 themed phishing emails to deceive individuals into divulging personal information or downloading malicious content. Additionally, it highlights instances where disruptive malware has been directed at critical infrastructure and medical organizations by these cybercriminals. Furthermore, the report underscores the growing incidents and dissemination of misinformation, which, in certain cases, contributes to the vulnerability exploited in cyber-attacks.

Hypothesis

A hypothesis refers to an idea or proposed explanation that serves as the initial point for further investigation, without any assumption of its truth based on limited evidence or reasoning. In essence, it is a tentative statement that is yet to be tested for validity. It may be either proven correct or incorrect, as it is based on suppositions that are provisionally accepted to interpret specific events or phenomena and to guide further investigation.

In the context of the present topic, the research hypothesis posits "***the need to strengthen and ensure effective implementation of cybercrime investigation techniques, effective restitution of victims, and prevention practices for cyber economic crimes in India."***

Research Questions

1. Whether there lies any specific difference between cybercrime in general and cyber economic offence in specific and types of such crime, if any?
2. What is the Indian legal framework for Cyber Economic Crime?
3. Whether there exist Indian legal framework for Cyber Crime Investigation and how it effectuated in practice?
4. What is Cyber Crime Investigation and how it is differ from traditional crime investigation?

5. What investigation techniques are deployed by Indian law enforcement agencies for investigation of cyber economic crime?
6. Which all law enforcement agencies and organization are involved in Cyber Crime Investigation, restitution of victims and its prevention?
7. Whether there is effective restitution of victims of cyber economic offence?
8. Whether exists proper and systematic legislative mechanism for restitution of cybercrime victims in India?
9. What is Cyber Crime prevention and what impact does it have on management of cyber economic offences?
10. How far India has progressed in Cyber Economic crime investigation, restitution of victims and cybercrime prevention in comparison to international scenario?

Research Methodology

The current research project adopts a Doctrinal or Non-empirical research methodology, which centers on legal doctrines, propositions, and the analysis of existing statutory provisions and case laws through the application of reasoning. The aim is to verify the hypothesis through legal reasoning and rational deduction, utilizing primary and secondary sources of law such as legislations, case laws, legal textbooks, commentaries, and official websites. Additionally, academic writings and newspaper reports are consulted to gain insights into the impact of cybercrimes. The utilization of this methodology serves the purpose of establishing legal principles for addressing the issue of cybercrimes at both the national and international levels. Ultimately, the research seeks to draw certain conclusions and provide recommendations based on its findings.

Scope and Limitations of Study

- The scope of the research is limited to the study of cyber economic crime in India with respect to the legislative mechanism and judicial approach.
- The research is focused on one component of the cybercrimes i.e., cyber economic crime and does not include other typologies of cybercrimes. The research is limited to the legal perspective and judicial approach towards cyber economic crime. Moreover, the study of cyber economic crime is limited to the country of India.

Scheme of Study

Tentative Chapters

CHAPTER 1: Introduction

This chapter will provide a concise overview of the research problem, a review of relevant literature, the rationale for conducting the research, and the research objectives. Additionally, the chapter will outline the research methodology employed and present a research design illustrating the overall flow of the study.

CHAPTER 2: Emergence of Cyber Economic Crime in India

Within this chapter, the focus will be on exploring the roots and causes of Cyber Economic Crime in India, as well as understanding its impact on the country. An analysis of relevant data will be included to gain insights into the extent and consequences of Cyber Economic Crime.

CHAPTER 3: Cyber Economic Crime – Investigative Methods and Techniques

This chapter will delve into the specialized investigative techniques employed in addressing cyber economic crime and cybercrime in general. It will also discuss the procedures and methodologies specific to investigating these types of crimes and highlight the differences compared to traditional crime investigation.

CHAPTER 4: Cyber Economic Crime – Indian Legal Framework and Judicial Approaches

In this chapter, a detailed discussion will be presented on the Information Technology Act, 2000, assessing its effectiveness in addressing cyber economic crime. The role and approaches of judicial bodies in handling such cases will also be examined and analyzed.

CHAPTER 5: Cyber Economic Crime - Prevention and Victim Restitution

This chapter will comprehensively explore preventive practices and frameworks for tackling cyber economic crime. Furthermore, the critical issue of restitution for victims affected by cyber economic crime will be analyzed, particularly considering the significant amount of public funds at stake.

CHAPTER 6: Stakeholders' Perspectives and Industry Expert Insights

Within this chapter, the opinions of stakeholders and industry experts will be discussed and analyzed. These insights will shed light on the realities faced in managing cyber economic crime, including

aspects relating to investigation, prosecution, victim restitution, and preventive measures. The chapter will also highlight gaps and shortcomings in the implementation of relevant laws and policies.

CHAPTER 7: Findings, Conclusions, and Recommendations

In this final chapter, an assessment will be made to determine whether the existing Indian legal framework and judicial approach adequately address the prosecution of cyber economic crime and restitution for victims. Furthermore, the effectiveness of current preventive practices for cyber economic crime will be assessed. Based on these findings, conclusions will be drawn, and suggestions for improvement will be provided.

References

Angkasa. (2018). Legal Protection for Cyber Crime Victims on Victimological aspect. *SHS Web of Conferences*.

Bakshi, P. M., & Suri, R. K. (2002). *Handbook of Cyber and E-Commerce Laws.* Bharat Publications House.

Britz, D. M. (2013). *Computer Forensics and Cyber Crime: An Introduction.* Pearson Education India.

Choudhary, J. N. (2020). Research, Training and Technology - Levers to Transform Policing in India. *The Indian Police Journal, 67-2*(ISSN 0537-2429).

Dasgupta, D. M. (2009). *Cyber Crime in India: A Comparative Study.* Eastern Law House Pvt Ltd.

DSCI - Paypal. (2020). *Fraud & Risk Management in Digital Payments.* DSCI - Paypal.

Duggal, P. (2008). *Cyber Law: The Indian Perspective.* Saakshar Law Publications.

Duggal, P. (2013). *Textbook on Cyber Law.* Universal Law Publishing Pvt Ltd.

Fatima, D. T. (2016). *Cyber Crimes.* Eastern Book Company.

Indian Evidence Act, 1872

Information Technology Act, 2000

In Re: *Dhyana Finstock Ltd.* SEBI WTM/RKA/ISD/59/2016

INTERPOL. (2020). *Cybercrime: COVID 19 Impact.* INTERPOL.

Iqbal, D. S. (2015). Cybercrime: A Technological Threat to the Society. *The Indian Policy Journal, LXII-1*(ISSN0537-2429).

Kamalakanta Tripathy vs State of Orissa &ors 2021 CriLJ 855

Kumar, M. (2020). A Detailed Study to Examine Digital Forensics and Cyber Security: Trends and Pattern in India. *International Journal of Forensic Sciences, 5*(2 ISSN: 2573-1734).

McGuire, D. M. (2018). *Into the Web of Profit: Understanding the Growth of the Cybercrime Economy.* Bromium Inc.

Mehta, D. S. (2012). Cyber Forensics and Amissibility of Digital Evidence. *SCC Online*.

Paranjape, D. V. (2010). *Legal Dimensions of Cybercrimes and Preventive Laws with Special Reference to India.* Central Law Agency Publication.

Prabhakar, A. (2020). Reforming Intelligence in 5GW. *The Indian Police Journal, 67-2*(ISSN 0537-2429).

Prakash Singh & ors vs Union of India & ors (2011) 14 SCC 21

Rai, R. (2015). Challenges to Cyber Crime Investigation - A need for Statutory Infrastructural Reforms. *SCC Online*(CNLU LJ (5) [2015] 62).

Reserve Bank of India. (2010). *Report of Working Committee on information security, electronic banking, technology risk management and cyber frauds.* Reserve Bank of India.

Ryder, R. D. (2007). *Guide to Cyber Laws (Information Technology Act, 2000 e-Commerce, Data Protection and the Internet).* Eastern Book Company.

Saxena, N. (2017). *Cyber Crime in India: Time Series Study of State Level data.* Manakin Press.

Seth, K. (2009). *Cyber Laws in the Information Technology Age.* Lexis Nexis Butterworth Wadhwa & Co.

Shamiulla, D. A. (2019). Virtual Surveillance of Cyber Crime and Accelerating Global Response: A Legal Perspective. *The Indian Police Journal, 66-2*(ISSN0537-2429).

Sharma, B. R. (2018). *Forensic Science in Criminal Investigation & Trials.* Universal Law Publishing.

Sharma, V. (2010). *Information Technology: Law and Practice.* Universal Law Publication Co.

Shibani Barik vs State of Orissa (2020) SCC Online Ori 425

Shreya Singhal vs Union of India AIR 2015 SC 1523

Singh, R. (2017). Efforts at Global Level to Combat Cyber Crimes - An Analysis. *SCC Online, 7*(GJLDP (April) 25).

Suman Kumar & ors vs Union Territory of Chandigarh CRM-M-14487/2020

*Touphik vs The State of Telangana&ors*W.P No. 2234 of 2021

Verma, D. A. (2009). *Cyber Crimes & Law.* Central Law House Publications.

Viswanathan, S. T. (2013). *The Indian Cyber Law.* Bharat Law House.

Wall, D. S. (2003). *Cybercrime: The Transformation of Crime in the Information Age.* Polity Press.

World Economic Forum. (2020). *Partnership against Cybercrime: Insight Report.* World Economic Forum.

Xie, S. L. (2011). Building Foundations for Digital Records Forensics: A Comparative Study of the Concept of Reproduction in Digital Records Management and Digital Forensics. *The American Archivist, 74*(2).

Research Scholar

Dr. Aseem chandra Paliwal
(Guide)